

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION  
3:15CV63

TECHNOLOGY PARTNERS, INC., )  
A North Carolina Corporation, and ICR DATA )  
CENTER, LLC, a North Carolina Limited )  
Liability Company, )  
 )  
Plaintiffs, )  
 )  
Vs. )  
 )  
IOANNIS PAPAIOANNOU, )  
 )  
Defendant. )  
\_\_\_\_\_ )

ORDER

This matter is before the Court upon Defendant's Motion for the Court to Take Judicial Notice, Rule 12(b)(6) Motion to Dismiss, and Motion for Attorney's Fees. These motions are fully briefed and ripe for disposition.

**FACTUAL BACKGROUND**

Plaintiff Technology Partners, Inc. ("TPI") is a business that has been providing workflow solutions and enterprise systems for the healthcare and life sciences business sector since the year 2000, including the development and sale of software to medical billing offices, medical practices, and hospitals. Compl. ¶ 7. In November of 2013, TPI formed ICR Data Center, LLC ("ICR") as a wholly owned subsidiary which operates a large group of computers that host applications and store data and documents exclusively for TPI and its customers. Compl. ¶ 10.

After TPI's founding, Defendant began working for TPI as a Network Engineer. Compl.

¶ 13. Plaintiffs allege that Defendant's position within TPI and ICR changed throughout his fourteen year tenure due to various negative performance issues—Defendant was first a Network Engineer, then Chief Information Officer, and finally ICR Data Center Director before his termination. Compl. ¶¶ 11 - 21. The Complaint alleges that while operating in each of these roles, TPI and ICR specifically and expressly limited Defendant's access to company data. Compl. ¶¶ 13, 16, 18, 20, 22. Due to repeated performance issues that were discussed in detail with Defendant, on or about November 3, 2014, Plaintiffs terminated his employment. Compl. ¶ 27. After Defendant's termination, Plaintiffs allege that they discovered (for the first time on February 3, 2015) numerous instances of Defendant's unauthorized access, theft, and large-scale deletion of TPI data. Compl. ¶¶ 29 - 30. Plaintiffs filed the instant action with this Court, alleging five claims for violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. The Complaint alleges that Defendant performed the following wrongful acts in violation of the CFAA: (1) deleting and intercepting emails belonging to other employees and to himself, some of which contained "proprietary financial data" (Compl. ¶¶ 31-40, 45-47); (2) deleting his "home directory" (Compl. ¶¶ 41-44); (3) forwarding TPI usernames and passwords to his personal email account (Compl. ¶¶ 48-50); and (4) hijacking TPI vendors and vendor information (Compl. ¶¶ 51-56). The Complaint further alleges state claims of Computer Trespass in violation of N.C. Gen. Stat. § 14-458(a), Unfair and Deceptive Trade Practices ("UDTPA"), and breach of contract. Defendant seeks to dismiss all of Plaintiffs' claims pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure.

## **DISCUSSION**

### **A. Standard of Review**

To survive a motion to dismiss under Fed. R. Civ. P. 12(b)(6), a complaint must “state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Id.* Moreover, while factual allegations set forth in the complaint are considered to be true, the same does not apply to legal conclusions set forth in the complaint. *Id.* at 678. Rather, plaintiffs must nudge their claims “across the line from conceivable to plausible [or] their complaint must be dismissed.” *Id.* at 680. “A pleading that offers ‘labels and conclusions’ or ‘a formulaic recitation of the elements of a cause of action will not do.’ Nor does a complaint suffice if it tenders ‘naked assertions’ devoid of ‘further factual enhancement.’” *Id.* at 678 (quoting *Twombly*, 550 U.S. at 555, 557).

### **B. The Computer Fraud and Abuse Act**

The CFAA permits a private party “who suffers damage or loss by reason of a violation of [the statute]” to bring a civil action “to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. § 1030(g). The CFAA makes an individual civilly liable if he (1) “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer,” in violation of § 1030(a)(2)(C); (2) “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value,” in violation of § 1030(a)(4); or (3) “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[,] or . . . causes damage and loss,” in violation of § 1030(a)(5)(B)-(C).

The trigger for liability under the CFAA in the Fourth Circuit is intentional “access” to a computer without authorization, or “exceed[ing] authorized access” to a computer, as outlined in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012). In *Miller*, WEC filed suit against a former employee, Miller, for violation of the CFAA after Miller allegedly stole confidential company information before he left WEC to work for a competitor. *Id.* at 202. As alleged in WEC’s complaint, while Miller worked for WEC, the company provided him with a laptop and complete unfettered access to the company’s intranet and computer servers. *Id.* WEC also instituted computer use policies that prohibited using confidential company data without prior authorization. *Id.* In its opinion, the Fourth Circuit noted that these computer use policies did not restrict Miller’s authorization to access the information, only to the use of the information. *Id.*

To determine the applicability of the CFAA to a defendant’s unauthorized access of a computer, the Fourth Circuit went to great lengths to define both “access” and “authorization.” In defining the words, the *Miller* court stated “‘access’ means ‘[t]o obtain, acquire,’ or ‘[t]o gain admission to’ [and] ‘authorization’ [means] ‘formal warrant, or sanction.’” *Id.* at 204. Therefore, the court concluded:

[A]n employee is authorized to access a computer when his employer approves or sanctions his admission to that computer. Thus, he accesses a computer “without authorization” when he gains admission to a computer without approval. Similarly, we conclude that an employee “exceeds authorized access” when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access.

*Id.* (citations omitted). After defining both “authorization” and “access,” the Fourth Circuit applied the CFAA to WEC’s complaint, concluding that WEC’s allegations alleged only that Miller violated the company’s computer use policy, and that because WEC specifically alleged in its complaint that Miller had unlimited access to WEC’s servers and confidential information,

the CFAA was inapplicable to Miller's actions. *Id.* 206 – 207. These allegations regarding violation of only WEC's computer use policy were the death knell to WEC's complaint, and the Fourth Circuit concluded, "WEC fails to allege that Miller and Kelley accessed a computer or information on a computer without authorization. . . . Thus, we agree with the district court that although Miller and Kelley may have misappropriated information, they did not access a computer without authorization or exceed their authorized access." *Id.* at 207.

Defendant argues that the present case is identical to the *Miller* case in that the Complaint does not contain allegations that the Defendant actually exceeded his *access*. In support of his argument, Defendant seeks to have the court take judicial notice of four exhibits consisting of pleadings and exhibits in the 2008 case of *Technology Partners, Inc. v. Hart*, 08-CVS-9873 and 3:08CV208 (the "Hart Case Documents").<sup>1</sup> Defendant contends that these documents, as well as the employment agreements attached to the Complaint, contradict the allegations in the Complaint, specifically the allegations that Defendant exceeded his authorized access to TPI computers in violation of the CFAA. Defendant claims the Hart Case Documents establish the following facts: (1) Defendant was Vice President of TPI; (2) Defendant was an Executive Officer of TPI; (3) Defendant had unlimited access to the confidential and trade secret information of TPI; and (4) Defendant was responsible for setting and ensuring the security of TPI passwords.

Federal Rule of Evidence 201 provides: "The court may judicially notice a fact that is not subject to reasonable dispute because it...can be accurately and readily determined from sources whose accuracy cannot be reasonably questioned." FED. R. EVID. 210(b)(2). The Fourth Circuit has held, "[i]n reviewing a Rule 12(b)(6) dismissal, we may properly take judicial notice of

---

<sup>1</sup> The Hart case arose when TPI filed suit against a former employee, Brian Hart, alleging a variety of claims resulting from his alleged misappropriation of confidential TPI information.

matters of public record. ... We may also consider documents attached to the complaint, *see* Fed. R. Civ. P. 10(c), as well as those attached to the motion to dismiss, so long as they are integral to the complaint and authentic.” *Phillips v. Pitt Cnty. Mem’l. Hosp.*, 572 F.3d 176, 180 (4th Cir. 2009) (citations omitted).

When applying the above rule to taking judicial notice of papers filed with courts in other legal proceedings, the Fourth Circuit has instructed courts to carefully consider whether the papers are integral to the complaint and authentic. If so, the court must then carefully consider the papers in a light most favorable to the plaintiff. “[W]hen a court considers relevant facts from the public record at the pleading stage, the court must construe such facts in the light most favorable to the plaintiffs.” *Zak v. Chelsea Therapeutics Int’l, Ltd.*, 780 F.3d 597, 607 (4th Cir. 2015). Moreover, “the determination whether a fact properly is considered under the [Federal Rule of Evidence 201] judicial notice exception depends on the manner in which a court uses this information.” *Id.* (citing *Clatterbuck v. City of Charlottesville*, 708 F.3d 549, 557 (4th Cir. 2013) (holding that the district court improperly considered contents of a public record as an established fact and as evidence contradicting the complaint)).

If a court does decide to take judicial notice of certain papers, it must be careful to limit that judicial notice so as to not take judicial notice of a party’s interpretation of those papers. *Ohio Valley Envtl. Coal. v. Aracoma Coal Co.*, 556 F.3d 177, 216 (4th Cir. 2009) (declining to take judicial notice of public documents and other exhibits because the party seeking notice sought “notice of its own interpretation of the contents of those documents” and not just notice of their existence). As the Fourth Circuit recently stated, “We are mindful that judicial notice must not ‘be used as an expedient for courts to consider matters beyond the pleadings and thereby upset the procedural rights of litigants to present evidence on disputed matters.’” *Goldfarb v.*

*Mayor & City Council of Baltimore*, 791 F.3d 500, 511 (4th Cir. 2015) (citing *Waugh Chapel S., LLC v. United Food & Commercial Workers Union Local*, 728 F.3d 354, 360 (4th Cir. 2013)).

The Hart Case Documents are simply not integral to the Complaint herein, nor are they explicitly relied upon. For that reason alone, the Court is not inclined to take judicial notice of the documents. Moreover, the Hart Case Documents do not directly contradict the allegations contained in Plaintiffs' Complaint, and do not establish the facts suggested by Defendant.

Exhibit 1 to Defendant's Motion to Dismiss, the complaint filed in the Hart Case, shows only that on April 28, 2008, Defendant was a Vice President of TPI. Plaintiffs contend that at the time there were several individuals that held the title of Vice President at TPI, including TPI's Vice President of Operations, Vice President of Business Development, Vice President of Sales, and Vice President of Software Engineering. Plaintiff's Complaint alleges that Defendant acted as a Network Engineer for TPI at this time. Compl. ¶ 16. It is certainly conceivable that Defendant held both titles. Exhibit 2 to Defendant's Motion to Dismiss, an affidavit signed by Defendant, establishes again that on May 1, 2008 Defendant was a Vice President of TPI.

Exhibit 3 to Defendant's Motion to Dismiss, a second affidavit signed by Defendant, establishes only that in 2008 Defendant had knowledge of various security measures used by TPI to protect its confidential information. Exhibit 4 to Defendant's Motion to Dismiss, TPI's response to Hart's first set of interrogatories, establishes again that on September 30, 2008 Defendant was a Vice President of TPI and that Defendant had knowledge of various security measures used by TPI to protect its confidential information. Nothing in the exhibits presented by Defendant necessarily "establish . . . that [Defendant] had unlimited access to the confidential and trade secret information of TPI," as suggested by Defendant.

Defendant asserts that Plaintiffs' allegations all pertain to Defendant's improper *use* of information validly accessed, and thus fail to state a claim for relief under the CFAA pursuant to *Miller*. However, even a cursory review of the Complaint reveals that Plaintiffs make numerous, specific allegations concerning (1) the specific scope of Defendant's data access privileges, and (2) Defendant's unauthorized access to Plaintiffs' computer systems that exceeded that specifically defined scope. *See e.g.*, Compl. ¶¶ 13, 16, 18, 20, 22, 30 - 56. For example, Plaintiffs allege that while employed as a Network Engineer for TPI, Defendant's data access privileges were limited in scope by TPI to include "solely the authority to access data relevant to the installation and maintenance the TPI network, and the authority to access TPI data that was directly relevant to the setup, design, and maintenance of the TPI network to ensure its operational effectiveness." Compl. ¶¶ 13, 16. Plaintiffs then allege that after Defendant's promotion to Chief Information Officer at TPI in 2009, his data access rights expanded. In addition to his previous access privileges as Network Engineer, Defendant "had administrative rights to all e-mail accounts within TPI for the purpose of ensuring operational effectiveness," and "TPI specifically and expressly limited Defendant's access within the TPI e-mail system, instructing Defendant that he may not access the e-mail content, attachments, or files of any TPI officer or employee. Defendant had no authority to access TPI computer system data outside this strict limitation." Compl. ¶¶ 18, 20. And finally, in January 2014 when TPI demoted Defendant due to poor performance, as alleged in the Complaint, Defendant's "data access privileges included solely the authority to access data relevant to the maintenance of the ICR data center and the creation of TPI client data backups." Compl. ¶ 22.

The Complaint reveals that Plaintiffs go to great lengths to not only define Defendant's scope of access, but also allege how he specifically exceeded and violated his scope of access.



Compl. ¶¶ 13, 16, 18, 20, 22, 30-56. At this stage in the litigation, these allegations are plausible and sufficient to withstand a motion to dismiss.

### **C. State Claims**

In addition to claims under the CFAA, Plaintiffs brought three claims under North Carolina law, including computer trespass, in violation of N.C. Gen. Stat. § 14-458(a); Unfair and Deceptive Trade Practices, in violation of N.C. Gen. Stat. § 75-1.1, *et seq.*; and breach of contract pursuant to Defendant's employment agreement with ICR. Defendant argues that these claims likewise fail pursuant to Rule 12(b)(6).

N.C. GEN. STAT. § 14-458(a) makes it a crime for any person to use a computer or computer network without authority and with the intent to, *inter alia*, temporarily or permanently remove or otherwise disable computer data, alter or erase computer data, or make or cause to be made an unauthorized copy of computer data.<sup>2</sup> A person is considered to be "without authority" within the meaning of the statute, "when (i) the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission." N.C. GEN. STAT. § 14-458(a). Defendant asserts that Plaintiffs' Complaint lacks any factual basis for the allegation that Defendant was "without authority" to access TPI's computer network. As explained above, however, the Court finds that Plaintiffs have sufficiently alleged that Defendant exceeded his access authority.

With respect to Plaintiffs' UDTPA claim, Defendant argues that this statute does not apply to the internal operations within a single business. In support of his argument, Defendant

---

<sup>2</sup> N.C. Gen. Stat. § 14-458(c) allows any person whose property is injured by reason of a violation of that section to recover damages.

cites *White v. Thompson*, 364 N.C. 47 (2010), in which the North Carolina Supreme Court established:

Our prior decisions have determined that the General Assembly did not intend for the [North Carolina unfair and deceptive trade practices] Act's protections to extend to a business's internal operations. As we determined in *Hajmm Co. [v. House of Raeford Farms, Inc.]*, 328 N.C. 578 (1991) and *Dalton [v. Camp]*, 353 N.C. 647 (2001), the Act is not focused on the internal conduct of individuals within a single market participant, that is, within a single business. To the contrary, as we observed in *Bhatti [v. Buckland]*, 328 N.C. 240 (1991) and *Sara Lee [Corp. v. Carter]*, 351 N.C. 27 (1999), the General Assembly intended the Act's provisions to apply to interactions between market participants. As a result, any unfair or deceptive conduct contained solely within a single business is not covered by the Act. As the foregoing indicates, this Court has previously determined that the General Assembly did not intend for the Act to intrude into the internal operations of a single market participant.

*White*, 364 N.C. at 53.

Defendant's conduct as alleged in the Complaint is confined to the internal operations of Plaintiffs and therefore fails to state a claim under the UDTPA. Defendant argues that this claim is frivolous and malicious and merits an award of attorney's fees pursuant to N.C. Gen. Stat. § 75-16.1. The Court disagrees. Defendant has failed to establish that this claim was brought in a malicious manner.

Lastly, Defendant contends that Plaintiffs' breach of contract claim fails because it contains only bare allegations of breach devoid of factual enhancement. Defendant's argument is without merit. Plaintiffs attached all relevant employment agreements to their Complaint. Compl. Exhibits A – D. These employment agreements include numerous clauses that require Defendant to comply with various affirmative contractual obligations, including the duty to comply with company policies, the duty to faithfully and diligently perform his duties, the duty to not only return all company data after termination, but the affirmative duty to preserve any

electronically stored communications belonging to Plaintiffs, a duty not to divulge Plaintiffs' confidential information, and a duty not to compete with Plaintiffs, among many others. *Id.*

Plaintiffs' Complaint generally alleges that Defendant's improper actions included the unauthorized access of TPI executive's e-mails to undertake theft of sensitive TPI financial data, the unauthorized mass deletion of Defendant's TPI e-mails and the e-mails of TPI high-ranking executives and employees, Defendant's mass deletion of his "home directory" on TPI's computer system, Defendant's secretive automatic forwarding and interception of e-mails sent to and from Mr. Khashman's wife's TPI e-mail account to himself, Defendant's forwarding of numerous sensitive TPI usernames and passwords to his own personal account, Defendant's substitution of his own personal contact information for that of TPI with numerous TPI vendors, including Dell, Microsoft, and other primary vendors, and Defendant's solicitation of prostitution utilizing Plaintiffs' resources. *See e.g.*, Compl. ¶ 30. These allegations are supported by specific dates and other details throughout Plaintiffs' Complaint. These allegations go well above and beyond the requirements of Fed. R. Civ. P. 8.

IT IS THEREFORE ORDERED that Defendant's Motion to Dismiss is hereby GRANTED IN PART AND DENIED IN PART. Plaintiffs' claim for Unfair and Deceptive Trade Practices is hereby dismissed; and

IT IS FURTHER ORDERED that Defendant's Motion for the Court to Take Judicial Notice and Motion for Attorney's Fees are hereby DENIED.

Signed: December 21, 2015



Graham C. Mullen  
United States District Judge

